Cybercrime, Cybersecurity & Cyberspace: LE Perspective

উপস্থাপনায়- **ইলিয়াস হোসেন**

পুলিশ পরিদর্শক(নিঃ)

স্পেশাল এ্যাকশন গ্রুপ

কাউন্টার টেরোরিজম এ্যান্ড ট্রান্সন্যাশনাল ক্রাইম

ডিএমপি, ঢাকা।

প্রাক্তন, ডিজিটাল ফরেনসিক এক্সপার্ট, সিআইডি, ঢাকা।

+৮৮০১৯১৯৯৩৩২২১

saymeonline@gmail.com

Education:

B. Ed (Hon's), M. Ed, PGDICT, MSc (Cyber Security), MHRL

Training Course completed:

1. Enhancement of Cybercrime investigation capability of Bangladesh Police, Soon Chung Hung University, South Korea, June 2014.2. Cyber Security Course, Gujarat 2. Forensic Science University, India 2016.
3. Exploit Hackers Tools & Technique, Singapore, October 2018.
4. Boot Camp on Access Data FTK, UAE Dubai, December 2018.
5. Windows Forensic, Singapore, March 2019.

Experience:

Serving as a Digital forensic Expert & Cyber Crime Investigator in Digital Forensics Forensic Lab from February 2012 to July 2021.

Experience as a Facilitator:

From 2013 to till today I have conducted training in different venues like Police Academy, Forensic Training Institute, Detective Training School, Cyber Crime Investigation Training Center.

UN Mission Experience:

Served as Police Advisor in the United Nations Mission in South Sudan from February 2017 to February 2018.

সাইবার ক্রাইম/ডিজিটাল অপরাধঃ

বাংলাদেশে প্রনীত তথ্য ও যোগাযোগ প্রযুক্তি আইন ২০০৬ (সংশোধনী/২০১৩), পর্নোগ্রাফী নিয়ন্ত্রন আইন ২০১২ এবং ডিজিটাল নিরাপত্তা আইন ২০১৮ এ বর্নিত শাস্তিযোগ্য সকল অপরাধই ডিজিটাল অপরাধ/সাইবার ক্রাইম।

ডিজিটাল অপরাধের ধরণঃ

আমাদের দেশে প্রচলিত **Digital** অপরাধগুলো হচ্ছে-

১। অশ্লীল ছবি/ভিডিও ধারণ, সংরক্ষণ, বিপনন, প্রদর্শণ করা।

২। সোস্যাল মিডিয়ায় মানহানিকর লেখা প্রচার/ছবি-ভিডিও আপলোড করা।

৩। সোস্যাল মিডিয়ার আইডি **Facebook/Twitter/Imo/ TikTok/Vigo/Viber/Tango/Mail Id/YouTube/ Web Site Hacking** (দখল) করা।

৪। **Fake Website** তৈরী করে প্রতারনা করা/ গ্রাহকের প্রকৃত তথ্যাদি নিয়ে **Real Website** প্রবেশ করে তথ্য চুরি/আর্থিক ক্ষতিসহ বিভিন্ন ধরণের অপরাধ করা।

৫। ভূয়া মেইল করে প্রতারণা করা/**Mail thread** করা।

৬। কম্পিউটার বা সার্ভার এর ডাটা বিনস্ট করা বা প্রোগ্রাম চেঞ্জ করা।

৭। মোবাইলের **Source Code /IMEI** পরিবর্তণ করা

৮। সোস্যাল মিডিয়াকে বিভিন্ন অপরাধের হাতিয়ার হিসেবে ব্যবহার করা (পরীক্ষার প্রশ্নপত্র ফাঁস/ গোপণ সংবাদ আদান-প্রদান করা)।

৯। অনলাইনে পণ্য ক্রয় করতে গিয়ে প্রতারণার ফাদে পরা।

১০। অনলাইনে পণ্য বিক্রয় করতে গিয়ে প্রতারণার ফাদে পরা।

১১। **Online Gaming/Gambling** সংক্রান্ত অপরাধ।

১২। **Virtual Currency/Cryptocurrency** সংক্রান্ত অপরাধ।

১৩। **ATM Card Fordgery** সংক্রান্ত অপরাধ।

১৪। **Mobile Banking (bkash/rocket/nagad)** প্রতারণা সংক্রান্ত অপরাধ।

১৫। **Mobile** থেকে **Mobile (SIM to SIM) SMS** পাঠিয়ে হুমকি বা বিরক্ত করা ।

১৬। **Online (যেকোন social media থেকে social media) Message** পাঠিয়ে হুমকি বা বিরক্ত করা।

১৭। **Copy Right** আইন লঙ্ঘন সংক্রান্ত অপরাধ।

১৮। **VOIP Calling** সংক্রান্ত অপরাধ।

Digital/Cyber অপরাধ নিয়ন্ত্রনে প্রনীত আইন সমূহ

১। তথ্য ও যোগাযোগ প্রযুক্তি আইন ২০০৬ (সংশোধনী/২০১৩)

২। পর্নোগ্রাফী নিয়ন্ত্রন আইন, ২০১২

৩। ডিজিটাল নিরাপত্তা আইন, ২০১৮

২০০৬ সালে আইন প্রণীত হলেও আমাদের সাইবার ক্রাইম সংক্রান্ত তদন্ত শুরু হয় ২০০৭ সালের শেষ দিকে। এই দীর্ঘ সময়ে আমাদের তদন্তের মান কাঙ্খিত পর্যায়ে পৌছায়নি।

আমাদের বর্তমান অবস্থা-

সাইবার অপরাধের শাস্তির হার মাত্র ৩%

সময়কাল	চার্জশীট প্রদান	চার্জ প্রমান	চার্জ প্রমান হয় নাই	শাস্তির হার
২০১৩-২০১৮	৪৯৫	১৫	৪৮০	৩%

Source: Dhaka Tribune- Published at 12:33 am April 20th, 2019

https://archive.dhakatribune.com/cybersecurity/2019/04/20/3-conviction-rate-of-cybercrime-in-bangladesh

Some Comments regarding this failure

Barrister Jyotirmoy Barua, with experience in a good number of cybercrime cases, said: **"The investigation**

Officers submit weak investigation reports due to poor knowledge. This is why it becomes difficult for the prosecution to prove charges."

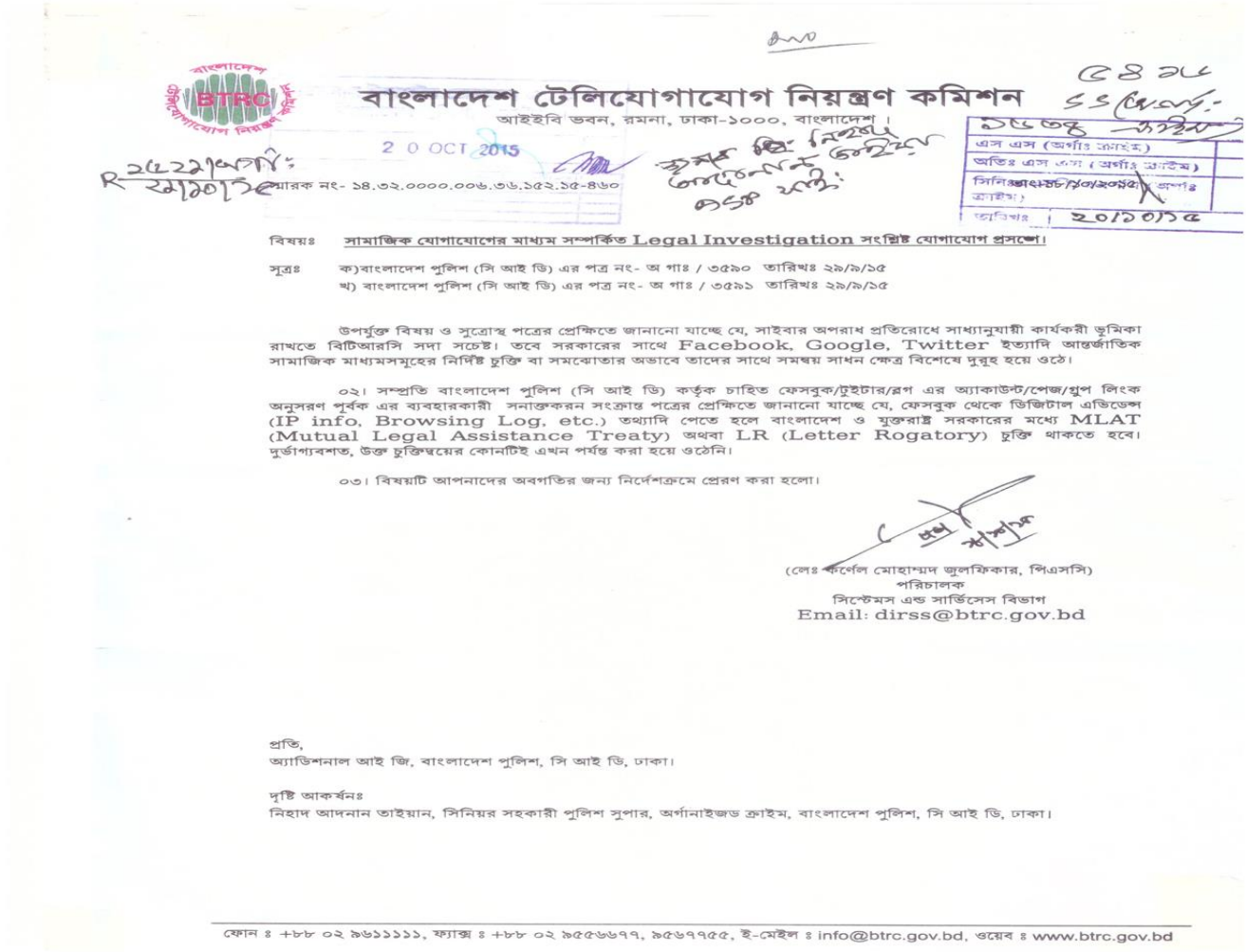
The legal expert also said most cases filed under the ICT Act are being filed just for harassment and the conviction rate is poor.

Advocate Nazrul Islam Shamim, a special public prosecutor for the Cyber Tribunal, said the **conviction rate was very poor due to out of court settlements, and faulty police probe reports due to lack of skills in handling digital crimes.**

He also said the **police often submits charge sheets in Cybercrime cases without IT and forensic reports.**

ব্যার্থতার কারন-

১. বাংলাদেশ সরকারের কোন সোস্যাল মিডিয়ার সাথে (Facebook, WhatsApp, Google) **MALT** (Mutual legal assistance treaty) **অথবা** LR (Letter rogatory) **চুক্তি এখন পর্যন্ত নাই, তবে চেষ্টা চলছে।**



বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশন
আইইবি ভবন, রমনা, ঢাকা-১০০০, বাংলাদেশ।

স্মারক নং- ১৪.৩২.০০০০.০০৬.৩৬.১৫২.১৫-৪৬০

20 OCT 2015

বিষয়ঃ সামাজিক যোগাযোগের মাধ্যম সম্পর্কিত Legal Investigation সংশ্লিষ্ট যোগাযোগ প্রসঙ্গে।

সূত্রঃ ক)বাংলাদেশ পুলিশ (সি আই ডি) এর পত্র নং- অ গাঃ / ৩৫৯০ তারিখঃ ২৯/৯/১৫
খ) বাংলাদেশ পুলিশ (সি আই ডি) এর পত্র নং- অ গাঃ / ৩৫৯১ তারিখঃ ২৯/৯/১৫

উপর্যুক্ত বিষয় ও সুত্রোস্থ পত্রের প্রেক্ষিতে জানানো যাচ্ছে যে, সাইবার অপরাধ প্রতিরোধে সাধ্যানুযায়ী কার্যকরী ভূমিকা রাখতে বিটিআরসি সদা সচেষ্ট। তবে সরকারের সাথে Facebook, Google, Twitter ইত্যাদি আন্তর্জাতিক সামাজিক মাধ্যমসমূহের নির্দিষ্ট চুক্তি বা সমঝোতার অভাবে তাদের সাথে সমন্বয় সাধন ক্ষেত্র বিশেষে দুরূহ হয়ে ওঠে।

০২। সম্প্রতি বাংলাদেশ পুলিশ (সি আই ডি) কর্তৃক চাহিত ফেসবুক/টুইটার/ব্লগ এর অ্যাকাউন্ট/পেজ/গ্রুপ লিংক অনুসরণ পূর্বক এর ব্যবহারকারী সনাক্তকরন সংক্রান্ত পত্রের প্রেক্ষিতে জানানো যাচ্ছে যে, ফেসবুক থেকে ডিজিটাল এভিডেন্স (IP info, Browsing Log, etc.) তথ্যাদি পেতে হলে বাংলাদেশ ও যুক্তরাষ্ট্র সরকারের মধ্যে MLAT (Mutual Legal Assistance Treaty) অথবা LR (Letter Rogatory) চুক্তি থাকতে হবে। দুর্ভাগ্যবশত, উক্ত চুক্তিদ্বয়ের কোনটিই এখন পর্যন্ত করা হয়ে ওঠেনি।

০৩। বিষয়টি আপনাদের অবগতির জন্য নির্দেশক্রমে প্রেরণ করা হলো।

(লেঃ কর্ণেল মোহাম্মদ জুলফিকার, পিএসসি)
পরিচালক
সিস্টেমস এন্ড সার্ভিসেস বিভাগ
Email: dirss@btrc.gov.bd

প্রতি,
অ্যাডিশনাল আই জি, বাংলাদেশ পুলিশ, সি আই ডি, ঢাকা।

দৃষ্টি আকর্ষনঃ
নিহাদ আদনান তাইয়ান, সিনিয়র সহকারী পুলিশ সুপার, অর্গানাইজড ক্রাইম, বাংলাদেশ পুলিশ, সি আই ডি, ঢাকা।

ফোন ঃ +৮৮ ০২ ৯৬১১১১১, ফ্যাক্স ঃ +৮৮ ০২ ৯৫৫৬৬৭৭, ৯৫৬৭৭৫৫, ই-মেইল ঃ info@btrc.gov.bd, ওয়েব ঃ www.btrc.gov.bd

২. ২০১৮ সালে সিআইডি, প্রধান কার্যালয় ঢাকাতে সাইবার পুলিশ ইনভেস্টিগেশন সেন্টার নামে একটি ইউনিট গঠন করা হয়, যাদের কাজ হচ্ছে সমগ্র বাংলাদেশে সংগঠিত সাইবার অপরাধের তদন্ত করা। ডিএমপি, ঢাকা সহ দেশের অন্যান্য মেট্রোপলিটন ইউনিটে এবং সিটিটিসি, ঢাকা'য় সাইবার ইউনিট রয়েছে। এছাড়াও পুলিশ হেডকোয়াটার্স, ঢাকায় নারীদের সহায়তার উদ্দ্যেশ্যে একটি হেল্পডেস্ক রয়েছে। সমস্যা হলো মামলার এজাহার দায়েরকালিন উল্লেখিত সংস্থার কোন দায়িত্ব নেই। ভুল বা সঠিক যেভাবেই

মামলার এজাহার দায়ের করা হোক না কেন তারা মামলা পরবর্তী সময়ে কিছু কিছু মামলার তদন্তের দায়িত্বভার তারা গ্রহন করে। থানা গুলোতে প্রশিক্ষিত বা প্রশিক্ষনবিহীন যাকে পাওয়া যায় তাকে দিয়েই বাদীর পক্ষে মামলার এজাহার দায়ের করা সহ প্রাথমিক কার্যক্রম সম্পন্ন করানো হয়। যে কারনে নিম্নোক্ত ভূলগুলো হয়ে থাকে।

(ক) এজাহার সঠিকভাবে নেওয়া হয়না।
(খ) অভিযুক্ত পোষ্ট (আপলোডকৃত ছবি/ ভিডিও/ লেখার স্ক্রিনশট) সঠিকভাবে নেওয়া হয়না।
(গ) মামলা সংশ্লিষ্ট আলামত জব্দ করা হয়না বা সঠিকভাবে করা হয়না।
(ঘ) অভিযুক্ত আইডি পরিচালনাকারী গ্রেফতার পরবর্তী সময়ে তার সোস্যাল মিডিয়ার আইডির কন্ট্রোল সঠিকভাবে নেওয়া হয় না।
(ঙ) ফরেনসিক মতামত সঠিকভাবে চাওয়া হয়না বা ফরেনসিক মতামত ছাড়াই চার্জশীট দেওয়া হয়।
৩। তদন্তকারী কর্মকর্তারা সাইবার ট্রাইবুনালে স্বাক্ষ্য প্রদানকালিন বিপক্ষ কৌশুলীর জেরার যথাযথ প্রতিউত্তর প্রদান করতে পারেন না।
৪। অধিকাংশ সাক্ষী বিজ্ঞ আদালতে সাক্ষ্য প্রদান কালিন যথাযথভাবে জিজ্ঞাসিত প্রশ্নের জবাব দিতে পারেন না।

আমাদের যা করতে হবে-

১। প্রয়োজনীয় সকল তথ্যাদি উল্লেখ পূর্বক এজাহার নিতে হবে।
২। অভিযুক্ত **Post** (ছবি/ভিডিও/লেখা/মন্তব্য) এর **Link** সহ **Screenshot** নিয়ে সাক্ষীদের সামনে জব্দ করতে হবে, কারণ এসব **Manipulate** করা যায় ।
৩। মামলা সংশ্লিষ্ট আলামত জব্দকালিন প্রতিটি আলামতের যথাযথ বর্ণনা জব্দ তালিকায় উল্লেখ করতে হবে।
৪। আসামী গ্রেফতার করতে পারলে আসামীর সহায়তায় অভিযুক্ত সংশ্লিষ্ট

সোস্যাল মিডিয়ার আইডিতে সর্তকতার সাথে প্রবেশ করে **Log in ID** জেনে **Password** পরিবর্তন করতে হবে এবং সংশ্লিষ্ট মোবাইল নম্বটির নিয়ন্ত্রন কোর্ট আদেশের মাধ্যমে নিতে হবে।

৫। সোস্যাল মিডিয়ায় অপরাধীর আইডি সঠিকভাবে চিহ্নিত করতে হবে এবং আইডির সাথে অপরাধীর (মোবাইল নম্বর/মেইল আইডি/ডিভাইস) যোগসূত্র খুঁজতে হবে।

৬। অভিযোগের বিষয় বস্তু যথাযথভাবে চিহ্নিতকরণপূর্বক মামলার আলামত হিসেবে জব্দ করতে হবে।

৭। অনেক আলামত বিশেষ করে মোবাইল ডিভাইস জব্দকালিন আমরা লক্ষ্য করি না যে, ডিভাইসটি **Lock (Pattern Lock/Pin Code Lock/Finger Lock/Eyerish Lock/Face Lock)** করা। জব্দকালিন ডিভাইস **Locked** থাকলে আসামীর সহায়তায় **Unlock** করে জব্দ করতে হবে।

৮। জব্দকৃত আলামতের ফরেনসিক পরীক্ষার মাধ্যমে আলামতের সাথে অভিযোগের সম্পৃক্ততা আছে কিনা/আলামত ব্যবহার করে অপরাধ করা হয়েছে কিনা সেই সম্পর্কে বিশেষজ্ঞ মতামত সুনির্দিষ্ট কর্তৃপক্ষের মাধ্যমে নিতে হবে।

৯। এই সকল মামলায় সাক্ষী হিসেবে অক্ষর জ্ঞান সম্পন্ন এমন কাউকে নির্বাচিত করতে হবে যে কিনা বিজ্ঞ কৌশলীর জেরার প্রশ্ন বুঝে সঠিকভাবে উত্তর দিতে সক্ষম।

১০। ফরেনসিক মতামত এবং অন্যান্য সাক্ষ্যের উপর ভিত্তি করে পুলিশ রিপোর্ট দাখিল করতে হবে।

মামলা পাওয়ার পরে সমসাময়িক গ্রহনযোগ্য পদ্ধতিতে তদন্ত কার্যক্রম এগিয়ে নিতে হবে। কোন ভাবেই তদন্তকালিন তদন্তের ধারাবাহিকতা থেকে বিচ্যুৎ হওয়া যাবেনা। তদন্তের মাধ্যমে অপরাধীকে চিহ্নিত করে সাক্ষ্য-প্রমান সংগ্রহ

করে পুলিশ রিপোর্ট দাখিলের মাধ্যমে শাস্তি নিশ্চিত করতে হবে। সব ক্ষেত্রে সফল হবেন না তবে তদন্ত কার্যক্রম গ্রহন যোগ্য হতে হবে।

Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These Cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

সাইবার নিরাপত্তা/সাইবার সিকিউরিটিঃ

সাইবার সিকিউরিটি/ সাইবার নিরাপত্তা হলো আমরা যে, সিস্টেম বা ডিভাইসের মাধ্যমে ইন্টারনেটে সংযুক্ত হয়ে কাজ করি সেই ডিভাইসে ব্যবহৃত ইন্টারনেট এবং প্রোগ্রামকে ডিজিটাল আক্রমন থেকে রক্ষা করার জন্য প্রয়োজনীয় নিরাপত্তামুলক সতর্কতা অবলম্বন করে কার্যক্রম চলমান রাখা।

Elements of Cyber Security

What are the 3 elements of Cyber security?

Elements of Cyber Security
The CIA triad refers to an information security model made up of the three main components: confidentiality, integrity and availability.

What are the four elements of security?

An effective security system comprises of four elements: Protection, Detection, Verification & Reaction.

What are the five elements of security?

It relies on five major elements: **confidentiality, integrity, availability, authenticity, and non-repudiation**.

Elements of Cyber Security

1. **Application Security**
2. **Information Security**
3. **Network Security**
4. **Disaster Recovery Planning**
5. **Operational Security.**
6. **End-user Security**
7. **Leadership commitment**

Application security

Applications play an essential role in business ventures; that is why every firm needs to focus on web application security. Having a secure web application is required to protect customers, their interests and their assets. Web application weakness or vulnerabilities is a common point of interference for a Cyber thief.

Information security

Information includes business records, personal data, customer's data, and intellectual property. For an organization, it is vital to have strong Cybersecurity for information as it is the heart of every organization.

Network Security

Network security consists of protecting the usability and reliability of network and data. A network penetration test is conducted to assess the

vulnerabilities in a system and other security issues which occur in servers, hosts, devices and network services.

Business continuity planning

Business continuity planning (BCP) is all about being prepared for interference or Cyber threat by identifying threats to the organization on time and analyzing how operations may be affected and how to overcome that.

Operational security

Operations security (OPSEC) is used to protect organization functions. It tracks critical information and assets to identify vulnerabilities that exist in the functional method.

End-user education

One of the standard errors that lead to data breaches is human error. Organization Cybersecurity is kept as strong as the weakest link. It is vital for an organization to train their employees about Cybersecurity. Every employee should be aware of the phishing attacks through emails and links and should have the potential to deal with Cyber threats they may face. The employee should share their device password with their co-workers and should not use an insecure network.

Leadership commitment

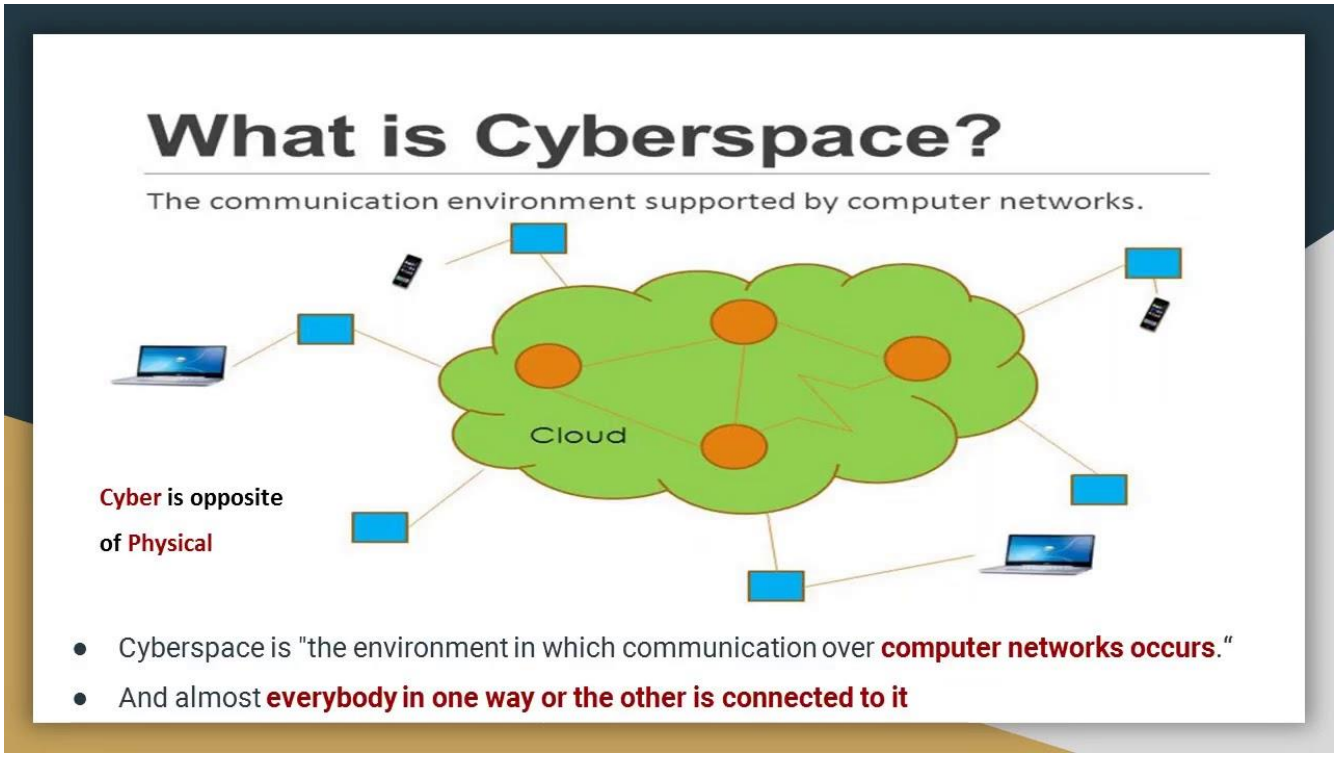
To have a successful Cybersecurity project, it is vital to have leadership commitment. Without having the leadership in the team it is complicated to develop, implement and maintain the processes.

The top leaders or management team an organization should invest in the Cybersecurity measures to make it useful and successful. With the support of leadership for Cybersecurity, an organization can improve investment in technology, resources, and skills.

Cyber Space

What exactly is cyberspace?

Cyberspace is a concept describing a widespread interconnected digital technology. The term cyberspace has become a conventional means to describe anything associated with the Internet and the diverse Internet culture.


What is Cyberspace?
The communication environment supported by computer networks.
Cloud
Cyber is opposite
of Physical
Cyberspace is "the environment in which communication over computer networks occurs."
And almost everybody in one way or the other is connected to it

সাইবার স্পেসঃ সাইবার স্পেস বলতে বুঝায় ইন্টারনেট সংযুক্ত একাধিক ডিজিটাল ডিভাইসের বিস্তৃতি পরিসরকে।

নারী সংক্রান্ত অভিযোগের জন্য

Police Cyber Support for Women – PCSW
https://www.facebook.com/PCSW.PHQ
cybersupport.women@police.gov.bd
Contact Number: 01320-000888

শুধু ঢাকা শহরের নাগরিকদের জন্য

Cyber Crime Investigation Division, CTTC, DMP
cyberhelp@dmp.gov.bd
https://www.facebook.com/cyberctdmp

সারাদেশের যেকোন জায়গার নাগরিকদের জন্য

Cyber Police Centre, CID, Bangladesh Police
Contact Number: 01320-010148,01730
cyber@police.gov.bd
https://www.facebook.com/cpccidbdpolice

সাইবার অপরাধ সম্পর্কে জানতে/বুঝতে ব্রাউজ করতে পারেন-

Bangladeshi website

https://dsa.gov.bd/
http://doict.portal.gov.bd/
https://ictd.gov.bd/
https://ccabd.org/
https://www.cirt.gov.bd/
https://www.bdcert.org/

International Website

https://www.unodc.org/unodc/en/cybercrime/index.html
https://portswigger.net/daily-swig
https://www.fbi.gov/investigate/cyber

-সবাইকে ধন্যবাদ আমাদের সাথে থাকার জন্য -